

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-298974

(43)Date of publication of application : 24.10.2000

(51)Int.Cl.

G11B 27/00
G06F 12/14

(21)Application number : 11-103130

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 09.04.1999

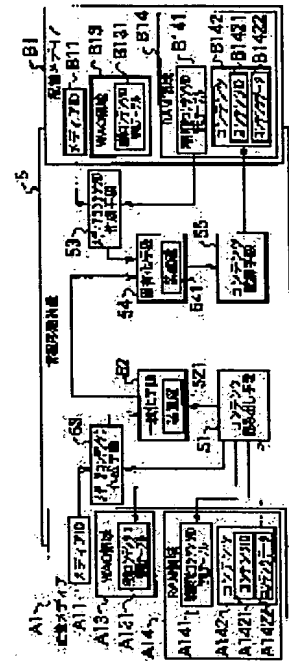
(72)Inventor : TAKEI HIDEAKI
SONEOKA AKINAO

(54) INFORMATION RECORDING METHOD CAPABLE OF MOVING INFORMATION MADE PECULIAR TO MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize an information recording method which moves information made peculiar to a storage medium to another storage medium while preventing the wrong use.

SOLUTION: When contents A141 are moved from a storage medium A1 to a storage medium B1, a contents read means 51 reads contents ID.A1421 in an ineffective contents ID management table of the storage medium A1, and contents data A1422 is recorded in the storage medium B1 as contents B142 through a generalizing means 52, a peculiarity making means 54, and a contents recording means 55, and contents A142 are deleted from the storage medium A1.



LEGAL STATUS

[Date of request for examination] 13.03.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

This Page Blank (uspto)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-298974

(P2000-298974A)

(43) 公開日 平成12年10月24日 (2000. 10. 24)

(51) Int. Cl. ⁷	識別記号	F I	テマコード* (参考)
G 1 1 B 27/00		G 1 1 B 27/00	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 D 1 1 0
		G 1 1 B 27/00	A

審査請求 未請求 請求項の数 3 O L (全 9 頁)

(21) 出願番号 特願平11-103130

(22) 出願日 平成11年4月9日 (1999. 4. 9)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 武井 英明

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 曾根岡 昭直

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100083806

弁理士 三好 秀和 (外1名)

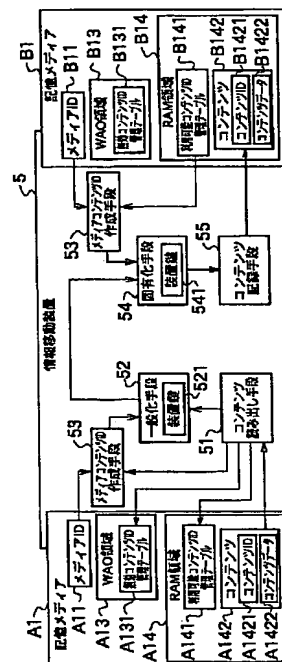
最終頁に続く

(54) 【発明の名称】 メディア固有化情報を移動可能にする情報記録方法

(57) 【要約】

【課題】 不正利用を防止しつつ記憶メディアに固有化された情報を他の記憶メディアに移動することを可能にするメディア固有化情報を移動可能にする情報記録方法を提供することにある。

【解決手段】 記憶メディアA1から記憶メディアB1にコンテンツA141を移動する際は、コンテンツ読み出し手段51は記憶メディアA1の無効コンテンツID管理テーブルに読み出したコンテンツID・A1421を記録し、コンテンツデータA1422は一般化手段52、固有化手段54、コンテンツ記録手段55を経てコンテンツB142として記憶メディアB1に記録し、コンテンツA142は記憶メディアA1から削除する。



【特許請求の範囲】

【請求項1】 一度だけ書き込み可能な記憶領域であるWAO領域および何度でも書き換え可能な記憶領域であるRAM領域を有するとともに、メディア毎に固有な識別子である書き換え不可能なメディアIDが書き込まれている記憶メディアに対して情報を記録する情報記録方法であって、

前記記憶メディアに目的情報を記録する際は、
前記記憶メディア内で利用できるコンテンツIDを検索し、
前記メディアIDと前記コンテンツIDを結合して、メディアコンテンツIDを生成し、
前記目的情報を前記メディアコンテンツIDで固有化してコンテンツデータを生成し、
前記コンテンツIDと前記コンテンツデータを組にしたコンテンツを前記記憶メディアの前記RAM領域に記録することを特徴とするメディア固有化情報を移動可能にする情報記録方法。

【請求項2】 前記記憶メディアにおいて今後使用できないコンテンツIDを管理するための無効コンテンツID管理テーブルを前記WAO領域に記録しておき、
前記記憶メディアに記録されている前記コンテンツを読み出し、この読み出したコンテンツから前記目的情報を取得する際は、
前記記憶メディアから読み出した前記コンテンツのコンテンツIDが前記無効コンテンツID管理テーブルに記録されているか否かをチェックし、記録されている場合には、目的情報の取得処理を中止し、
前記コンテンツのコンテンツIDが前記無効コンテンツID管理テーブルに記録されていない場合には、前記メディアIDと前記コンテンツIDを結合して、メディアコンテンツIDを生成し、
この生成したメディアコンテンツIDで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得することを特徴とする請求項1記載のメディア固有化情報を移動可能にする情報記録方法。

【請求項3】 前記記憶メディアにおいて今後使用できないコンテンツIDを管理するための無効コンテンツID管理テーブルを前記WAO領域に記録しておき、
前記記憶メディアにおいて利用できるコンテンツIDを管理するための利用可能コンテンツID管理テーブルを前記RAM領域に記録しておき、
第1の記憶メディアから第2の記憶メディアに前記コンテンツを移動する際は、
前記第1の記憶メディアから前記コンテンツを読み出し、
この読み出したコンテンツのコンテンツIDが前記第1の記憶メディアの前記無効コンテンツID管理テーブルに記録されていないことを確認してから、該コンテンツIDを該無効コンテンツID管理テーブルに記録すると

ともに、該コンテンツIDを前記第1の記憶メディアの前記利用可能コンテンツID管理テーブルから削除し、
前記第1の記憶メディアの第1のメディアIDと前記読み出したコンテンツのコンテンツIDを結合して、第1のメディアコンテンツIDを生成し、
この第1のメディアコンテンツIDで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得し、
前記第2の記憶メディアの第2のメディアIDと前記コンテンツIDを結合して、第2のメディアコンテンツIDを生成し、
前記第1の記憶メディアから取得した目的情報を前記第2のメディアコンテンツIDで固有化してコンテンツデータを生成し、
前記コンテンツIDと前記コンテンツデータを組にしたコンテンツを前記第2の記憶メディアの前記RAM領域に記録し、
前記第1の記憶メディアのRAM領域に記録されている前記コンテンツを消去することを特徴とする請求項1記載のメディア固有化情報を移動可能にする情報記録方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、メディア毎に固有な識別子であるメディアIDを有する記憶メディアに対して情報を固有化し、この固有化されている情報を記憶メディアから読み出し、更に他の記憶メディアに移動するとともに情報の不正利用を適確に防止し得るメディア固有化情報を移動可能にする情報記録方法に関する。

【0002】

【従来の技術】まず、情報の固有化および一般化という用語について説明する。以下では暗号鍵KでデータDを暗号化することをE(K, D)と表現する。

【0003】不正利用を防ぐためによく用いられるのは、情報を記録したり利用する装置間で共有され、かつ利用者には秘密にされている秘密鍵を使う方法である。この秘密鍵のことを装置鍵Rと呼ぶ。

【0004】更に、情報をメディアに固有化することで、情報を他のメディアにコピーしても、他のメディアでは情報を適切に復号化できないため不正利用を防ぐことが可能になる。その1つの例がメディア毎に固有な識別子を利用した方法である。メディア毎に固有な識別子を利用した方法を以下で簡単に説明する。

【0005】各メディアには、予めメディア毎に固有な識別子(メディアID)が書き換え可能なように書き込まれている。従って、2つのメディアがあったときに、この2つのメディアのそれぞれのメディアIDが一致することはない。このようなメディアに対して不正利用を防止しようとする目的情報Cを記録するときには、まずメディアID(MI)を装置鍵Rで暗号化しE(R, M

10

20

30

40

50

I)を得る。これを暗号鍵として目的情報Cを暗号化して生成される暗号化目的情報E (E (R, MI), C)をメディアは書き込むのである。

【0006】一方この目的情報Cを読み出すときには、記録されている暗号化目的情報E (E (R, MI), C)とメディアID (MI)を読み出し、MIを装置鍵Rで暗号化してE (R, MI)を得て、これを復号鍵としてE (E (R, MI), C)を復号化して目的情報Cを得ることができる。

【0007】このとき、あるメディアAに記録されている暗号化目的情報を別のメディアBにコピーし、メディアBからこの暗号化目的情報を読み出すことを考える。このとき、メディアAのメディアID (MIA)とメディアBのメディアID (MIB)は異なる。従って、メディアBにコピーされた暗号化目的情報を上記のように読み出そうとしても、暗号化に用いた鍵 (E (R, MIA))と復号化に用いる鍵 (E (R, MIB))が異なるため、目的情報を正確に読み出すことはできない。つまりこの暗号化目的情報は、メディアAに記録されているときのみ有効な情報であり、他のメディアに記録されているときは無効な情報となる。これを目的情報のメディアへの固有化と呼ぶ。情報をメディアに固有化することにより、情報を他のメディアにコピーしても利用することが不可能になり、不正利用を防いでいるのである。

【0008】また、暗号化目的情報E (E (R, MI), C)を生成するには、メディアID (MI)と目的情報Cの他に装置鍵Rを知る必要がある。逆に、暗号化目的情報E (E (R, MI), C)を復号化するには、メディアID (MI)の他に装置鍵Rを知ることが必要になる。従って装置鍵Rが秘密に守られているならば、メディアIDを知られたからといって、不正に暗号化目的情報を生成したり、暗号化目的情報から目的情報を生成することはできない。

【0009】以上説明したように、情報をメディアに固有化することは不正利用の防止を実現するのに強力な方法となる。別の言い方をすると、メディア内の情報はそのメディアに固有化されているため、メディア内の情報がたとえコピーされたとしても、それは不正利用防止方法への脅威とはならない。その固有化された情報はそのメディアに記録されているときのみ適切に復号化され意味のあるものになるのであり、他のメディアに記録されているときはまったく無意味なものであるからである。つまりメディアに固有化された情報を利用するためには、そのメディアを物理的に所有する必要がある。情報を利用する権利が物理的なメディアの所有に結び付けられているのである。

【0010】そこで、メディアID (MI)と目的情報Cから固有化目的情報E (E (R, MI), C)を生成することを目的情報をメディアIDで固有化すると表現し、固有化目的情報とメディアIDから目的情報を生成

することを固有化目的情報をメディアIDで一般化すると表現する。

【0011】以上の説明から明らかなように、メディア内の固有化情報を他のメディアにコピーされても不正利用を防止する上で問題はない。従って利用者はメディア内の固有化情報を例えばハードディスク、MOなどの別のメディアにバックアップとして記録することができる。利用者は、記憶メディア内に多量の情報がたまってきて、残りの記憶容量が少なくなってきたとき、そのうちのいくつかをバックアップとして別の記録媒体にコピーしてとっておき、その記憶メディア内の情報を削除すれば、残りの記憶容量を増やすことができる。必要になればバックアップから記憶メディアに情報をコピーして戻せばよい。戻した情報は有効な情報として利用することが可能である。このように利用者が合法的にいくつでも情報のバックアップをとっておけるということは利用者にとって大変便利なことである。

【0012】ところで、このような従来の方法では、利用するために記憶メディアに記録してしまった情報を他の記憶メディアで利用するために情報を移動することができず、その点では利用者は不便を強いられてしまう。これはバックアップのことを言っているのではなく、別のメディアに情報をコピーし、その別なメディア上で情報を利用することを許すと不正利用の余地が生まれるということを言っているのである。

【0013】情報の移動とは、例えばメディアAからメディアBに情報を移すことである。利用者は2つのメディアに入っている別々の情報を1つのメディアにまとめることができれば便利であり、このとき情報の移動をすることが必要になる。情報の移動において不正利用を防止するという観点から重要なのは、例えばメディアAからメディアBに情報を移すときにメディアA内の情報を後から使えないようにするということである。つまり情報の移動とは、メディアAに固有化されている情報をメディアBに固有化しなおすという作業であり、移動前はメディアAと結び付けられていた情報を利用する権利を移動してメディアBと結び付ける作業であるといえる。

【0014】メディア間で移動するためには、以下の方法が容易に考えられる。まずメディアA内の固有化された情報を一般化する。この一般化された情報をメディアBに固有化し、メディアBに記録する。そしてメディアA内の固有化された情報を消去する。このような機能を利用者に提供すれば、とりあえず、メディア間の固有化情報の移動が実現できる。

【0015】しかし、ここで問題となるのは、利用が許されないメディアA内の情報が、確実に利用できないになっているのかということである。例えば利用者が移動の作業をする前にメディアA内の情報を予めバックアップしていた場合を考える。移動の作業が終了した後は、メディアA内の情報は上記のように消去されるから

確かにメディアA内には移動した情報は残っていない。しかし、予めバックアップをとっていたなら、このバックアップをまたメディアAにコピーして戻してしまえば、この情報は有効であり、利用できるようになってしまう。

【0016】バックアップを禁止することでこのような不正利用を防止することができるが、バックアップを防止する技術を開発することは、特に単に記録するだけの単純な記憶メディアの場合には困難である。更に、何よりバックアップはそれ自体便利な機能であり、これを禁止することは利用者にとって大変不便である。

【0017】以上のように、従来の技術では、メディア内の情報を他のメディアに移動する機能を利用者に提供した場合、利用者は情報を不正にコピーして利用することが容易になってしまう。

【0018】

【発明が解決しようとする課題】上述したように、メディアに固有化された情報を他のメディアに移動させることを実現しようとする、情報の移動後にバックアップをメディアにコピーしなおすことで容易に不正利用が行われてしまうという問題がある。

【0019】バックアップを防止することで不正利用を防ぐことができるが、バックアップを防止することは利用者の利便性を損なうという問題がある。

【0020】本発明は、上記に鑑みてなされたもので、その目的とするところは、記憶メディアに固有化されている情報を異なる記憶メディアに移動することでバックアップを可能にしつつ不正コピーによる情報の不正利用を適確に防止し得るメディア固有化情報を移動可能にする情報記録方法を提供することにある。

【0021】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、一度だけ書き込み可能な記憶領域であるWAO領域および何度でも書き換え可能な記憶領域であるRAM領域を有するとともに、メディア毎に固有な識別子である書き換え不可能なメディアIDが書き込まれている記憶メディアに対して情報を記録する情報記録方法であって、前記記憶メディアに目的情報を記録する際は、前記記憶メディア内で利用できるコンテンツIDを検索し、前記メディアIDと前記コンテンツIDを結合して、メディアコンテンツIDを生成し、前記目的情報を前記メディアコンテンツIDで固有化してコンテンツデータを生成し、前記コンテンツIDと前記コンテンツデータを組にしたコンテンツを前記記憶メディアの前記RAM領域に記録することを要旨とする。

【0022】請求項1記載の本発明にあっては、メディアIDとコンテンツIDを結合してメディアコンテンツIDを生成し、目的情報をメディアコンテンツIDで固有化してコンテンツデータを生成し、コンテンツIDと

コンテンツデータを組にしたコンテンツを記憶メディアに記録するため、メディアIDをコンテンツIDで暗号化した結果で目的情報を固有化し得るとともに、また予め別のコンテンツ鍵を用意し、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を目的情報として固有化することによりコンテンツの暗号化の処理を軽減することも可能である。

【0023】また、請求項2記載の本発明は、請求項1記載の発明において、前記記憶メディアにおいて今後使用できないコンテンツIDを管理するための無効コンテンツID管理テーブルを前記WAO領域に記録しておき、前記記憶メディアに記録されている前記コンテンツを読み出し、この読み出したコンテンツから前記目的情報を取得する際は、前記記憶メディアから読み出した前記コンテンツのコンテンツIDが前記無効コンテンツID管理テーブルに記録されているか否かをチェックし、記録されている場合には、目的情報の取得処理を中止し、前記コンテンツのコンテンツIDが前記無効コンテンツID管理テーブルに記録されていない場合には、前記メディアIDと前記コンテンツIDを結合して、メディアコンテンツIDを生成し、この生成したメディアコンテンツIDで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得することを要旨とする。

【0024】請求項2記載の本発明にあっては、コンテンツのコンテンツIDが無効コンテンツID管理テーブルに記録されている場合には、目的情報の取得処理を中止し、記録されていない場合には、メディアIDとコンテンツIDを結合してメディアコンテンツIDを生成し、このメディアコンテンツIDでコンテンツのコンテンツデータを一般化して、目的情報を取得するため、無効になって、無効コンテンツID管理テーブルに記録されているコンテンツの目的情報は取得できないとともに、更にメディアIDをコンテンツIDで暗号化した結果でコンテンツデータを一般化することができる。なお、コンテンツに含まれるコンテンツIDについては暗号化してなく、コンテンツIDを不正に別の値にすることにより、コンテンツを本来のコンテンツIDとは別のコンテンツIDを有するコンテンツにされる恐れがあるが、コンテンツに含まれるコンテンツデータとしてはコンテンツIDを含む値で固有化したデータが記録されており、コンテンツデータはコンテンツIDに依存している。この場合、上述したようにコンテンツデータを読み出すときには、本来のコンテンツIDでないIDを含む値でコンテンツデータを一般化するため、読み出しの結果得られる情報は本当の正直な情報ではなく、無意味な情報となる。従って、コンテンツIDを本来のものから変えても得られる情報が無意味になるだけである。

【0025】更に、請求項3記載の本発明は、請求項1記載の発明において、前記記憶メディアにおいて今後使用できないコンテンツIDを管理するための無効コンテ

ンツID管理テーブルを前記WAO領域に記録しておき、前記記憶メディアにおいて利用できるコンテンツIDを管理するための利用可能コンテンツID管理テーブルを前記RAM領域に記録しておき、第1の記憶メディアから第2の記憶メディアに前記コンテンツを移動する際は、前記第1の記憶メディアから前記コンテンツを読み出し、この読み出したコンテンツのコンテンツIDが前記第1の記憶メディアの前記無効コンテンツID管理テーブルに記録されていないことを確認してから、該コンテンツIDを該無効コンテンツID管理テーブルに記録するとともに、該コンテンツIDを前記第1の記憶メディアの前記利用可能コンテンツID管理テーブルから削除し、前記第1の記憶メディアの第1のメディアIDと前記読み出したコンテンツのコンテンツIDを結合して、第1のメディアコンテンツIDを生成し、この第1のメディアコンテンツIDで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得し、前記第2の記憶メディアの第2のメディアIDと前記コンテンツIDを結合して、第2のメディアコンテンツIDを生成し、前記第1の記憶メディアから取得した目的情報を前記第2のメディアコンテンツIDで固有化してコンテンツデータを生成し、前記コンテンツIDと前記コンテンツデータを組にしたコンテンツを前記第2の記憶メディアの前記RAM領域に記録し、前記第1の記憶メディアのRAM領域に記録されている前記コンテンツを消去することを要旨とする。

【0026】請求項3記載の本発明にあっては、第1の記憶メディアから第2の記憶メディアに前記コンテンツを移動する際は、第1の記憶メディアから読み出したコンテンツのコンテンツIDが第1の記憶メディアの無効コンテンツID管理テーブルに記録されていないことを確認し、第1の記憶メディアの第1のメディアIDとコンテンツIDを結合して第1のメディアコンテンツIDを生成し、この第1のメディアコンテンツIDでコンテンツのコンテンツデータを一般化して、目的情報を取得するとともに、第2の記憶メディアの第2のメディアIDとコンテンツIDを結合して第2のメディアコンテンツIDを生成し、第1の記憶メディアから取得した目的情報を第2のメディアコンテンツIDで固有化してコンテンツデータを生成し、コンテンツIDとコンテンツデータを組にしたコンテンツを第2の記憶メディアに記録するため、無効コンテンツID管理テーブルに記録されているコンテンツの目的情報は取得できず、従って移動前に予め第1の記憶メディアのコンテンツをバックアップしてあった場合、移動の際にコンテンツのコンテンツIDは無効にされるため、移動後にバックアップを第1の記憶メディアにコピーして、上述したように読み出して利用しようとしてもコンテンツを読み出すことはできない。なお、この場合、バックアップすること自体は禁止していない。すなわち、バックアップを許容しつつコ

ンテンツ移動後にバックアップを記憶メディアにコピーして戻した場合に、このコンテンツを利用できないようにしているのである。

【0027】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。図1は、本発明の第1の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。同図に示すシステムは、記憶メディア1、およびこの記憶メディア1に対して不正利用を防止しつつ目的情報3を記録するための情報記録装置2を有する。

【0028】記憶メディア1は、記憶メディア毎に固有な識別子であって、書き換え不可能なメディアID11、一度だけ書き込み可能な記憶領域であるWAO（Write At Once）領域13、および何度でも書き換え可能な記憶領域であるRAM（Read Only Memory）領域14を有する。WAO領域13は、無効コンテンツID管理テーブル131を有する。

【0029】ここで、WAO領域13の性質について説明する。このWAO領域13には情報を一度だけ書き込むことができる。一度書き込んだ情報を元に戻すことはできない。また、この書き込む情報の最小単位はビットであり、1ビット単位で情報を書き込むことができる。

【0030】例をあげて説明する。8ビットのWAO領域を考える。最初はすべて「0」であり、すべてのビットが書き込み可能である。

【0031】「00000000」次に、4ビット目を「1」にしてみる。これは可能である。

【0032】「00010000」この4ビット目の「1」は以後いかなることをしても「0」にできない。

これはWAO領域の性質である。

【0033】更に別のビットを「1」にすることができる。例えば7ビット目を「1」にすると、「00010010」となる。このようにして書き込みを行っていくと、やがてすべて「1」の状態、「11111111」になる。この状態からは以後いかなることをしても状態を変化させることはできない。

【0034】RAM領域14は、利用可能コンテンツID管理テーブル141と複数のコンテンツ142を有する。利用可能コンテンツID管理テーブル141は、コンテンツを利用する権利を保持したままコンテンツを他へバックアップし記憶メディア1からはコンテンツを消去してしまう場合に、それ以後に記憶メディア1に新しく記録するコンテンツに対して、バックアップして消去してしまったコンテンツのコンテンツIDが使われてしまうことを防ぐために使用される。コンテンツ142はコンテンツID1421とコンテンツデータ1422を有する。

【0035】情報記録装置2は、記憶メディア1からメディアID11と利用可能コンテンツID管理テーブル

141から利用可能なコンテンツID1421の2つの要素を入力とし、2つの入力を結合した結果を出力とするメディアコンテンツID作成手段21と、メディアコンテンツID作成手段21から出力されるメディアコンテンツIDで目的情報3を固有化する固有化手段22と、コンテンツID1421とコンテンツデータ1422からなるコンテンツ142をRAM領域14に記録するコンテンツ記録手段23を有する。また、固有化手段22は装置鍵221を有する。

【0036】図2は、無効コンテンツID管理テーブル131のフォーマットを示している。単純なビット列であり、各ビットが対応するコンテンツIDが無効であるか否かを示している。テーブル131のビットとコンテンツIDとの対応は、ビット列の先頭からのオフセット距離がコンテンツIDの番号と一致するように対応付ける。ビットの値の初期値は0であり、コンテンツIDが無効となったとき対応するビットは1にされる。図2に示す無効コンテンツID管理テーブル131では、コンテンツIDが8と13が無効であることを示している。無効コンテンツID管理テーブル131の大きさを16

KByteとすると、 $16 \times 1024 \times 8 = 131072$ 個のコンテンツIDを管理することができる。記憶メディア1の出荷時における無効コンテンツID管理テーブル131の初期値はすべて0である。無効コンテンツID管理テーブル131はWAO領域13上に記録されるため、一度1にしたビットは二度と0にできない。従って、無効コンテンツID管理テーブル131からはいかなるコンテンツIDも削除できない。

【0037】利用可能コンテンツID管理テーブル141のフォーマットは無効コンテンツID管理テーブル131と同一であり、テーブルの大きさも同じとする。記憶メディア1の出荷時における利用可能コンテンツID管理テーブル141の初期値はすべて1である。

【0038】なお、以降の処理において、これらコンテンツID管理テーブルにコンテンツIDを記録すると、そのコンテンツIDに対応するテーブル中のビットを1にすることを意味する。コンテンツID管理テーブルからコンテンツIDを削除するとは、そのコンテンツIDに対応するテーブル中のビットを0にすることを意味する。

【0039】以上のように構成される第1の実施形態において、目的情報C3を記憶メディア1に記録する場合には、まずメディアコンテンツID作成手段21によって記憶メディア1からメディアID(MI)11と、利用可能コンテンツID管理テーブル141から利用可能なコンテンツIDを検索した結果のコンテンツID(CI)の2つの入力から、メディアコンテンツID(MCI)を生成する。 $MCI = MI + CI$ である。このときコンテンツID(CI)は利用可能コンテンツID管理テーブル141から削除する。

【0040】次に、固有化手段22が目的情報CをメディアコンテンツIDで固有化して固有化情報を生成する。装置鍵221をRとすると、この固有化情報は、 $E(E(R, MCI), C)$ と表現される。最後にCIをコンテンツID1421に、固有化情報E($E(R, MCI), C$)をコンテンツデータ1422としたコンテンツ142をコンテンツ記録手段23によって記憶メディア1のRAM領域14に記録する。

【0041】図3は、本発明の第2の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図3に示すシステムは、記憶メディア1と、記憶メディア1から情報を読み出す情報利用装置4と、目的情報3を有する。記憶メディア1の構成は図1と同じである。

【0042】情報利用装置4は、記憶メディア1からコンテンツ142を読み出し、更に読み出したコンテンツ142のコンテンツID1421が無効コンテンツID管理テーブル131に含まれているかどうかを検査するコンテンツ読み出し手段41と、メディアコンテンツID作成手段43と、メディアコンテンツID作成手段43から出力されるメディアコンテンツIDでコンテンツデータ142を一般化する一般化手段42を有する。また、一般化手段42は装置鍵421を有する。一般化手段42内の装置鍵421は前述の固有化手段22内の装置鍵221と同一である。

【0043】記憶メディア1からコンテンツ142を読み出す場合について説明する。この説明では第1の実施形態で書き込んだ記憶メディア1とコンテンツ142を用いる。すなわち、コンテンツID1421はCI、コンテンツデータ1422は $E(E(R, MCI), C)$ であるとし、メディアID11はMIとする。まず、コンテンツ読み出し手段41によってコンテンツ142を読み出し、コンテンツID(CI)とコンテンツデータ $E(E(R, MCI), C)$ を読み出す。更にコンテンツ読み出し手段41は、この読み出したコンテンツID(CI)が無効コンテンツID管理テーブル131に含まれていないか検査する。含まれていない場合は、ただちに動作は終了となる。含まれていない場合は、動作を続行し、メディアコンテンツID作成手段43によって、コンテンツID(CI)とメディアID11(MI)からメディアコンテンツID($MI + CI = MCI$)を生成し、更に一般化手段42を用いて、コンテンツデータ $E(E(R, MCI), C)$ をメディアコンテンツID(MCI)で一般化し、目的情報Cを得る。

【0044】図4は、本発明の第3の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図4に示すシステムは、記憶メディアA1と、記憶メディアB1と、記憶メディアA1から記憶メディアB1に情報を移動する情報移動装置5を有する。記憶メディアA1、B1の構成は図1、図3に示したものと同

じである。

【0045】情報移動装置5はコンテンツ読み出し手段51と、一般化手段52と、メディアコンテンツID作成手段53と、固有化手段54と、コンテンツ記録手段55を有する。一般化手段52内の装置鍵521は固有化手段54内の装置鍵541と同一である。

【0046】記憶メディアA1から記憶メディアB1にコンテンツを移動する場合を説明する。コンテンツ読み出し手段51、メディアコンテンツID作成手段53、一般化手段52の動作は、第2の実施形態と一部の例外を除き同一の動作をする。その例外とは、コンテンツ読み出し手段51は読み出したコンテンツID・A1421を利用可能コンテンツID管理テーブルA141から削除する（対応ビットを1→0にすること、同じくコンテンツID・A1421を無効コンテンツID管理テーブルA131に記録する（対応ビットを0→1にすること、更にコンテンツA142がRAM領域A14から削除されることである。このようにして、一般化手段52は一般化情報を生成し、固有化手段54に渡す。以下、固有化手段54、メディアコンテンツID作成手段53、コンテンツ記憶手段55の動作は、第1の実施形態と同一の動作をする。このようにして、コンテンツB142が記憶メディアB1に記録される。

【0047】図5は、本発明の第4の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図5に示すシステムは、記憶メディア1と、バックアップ装置6と、磁気ディスク7を有する。バックアップ装置6にコンテンツ読み出し手段61と、コンテンツ記録手段62を有する。なお、記憶メディア1の構成は、一部省略されているが、図1、図3、図4に示したものと同一である。

【0048】記憶メディア1から磁気ディスク7にコンテンツのバックアップをとる際は、コンテンツ読み出し手段61がコンテンツ142を読み出し、これを磁気ディスク7に記録する。また、磁気ディスク7から記憶メディア1にバックアップしたデータをコピーして戻す（リストア）する場合は、コンテンツ記録手段62が磁気ディスク7からデータを読み出し、これをコンテンツ142としてRAM領域14に記録する。

【0049】図6は、本発明の第5の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図6に示すシステムは、記憶メディア1と、削除装置8を有する。削除装置8はコンテンツ削除手段81を有する。なお、記憶メディア1の構成は、一部省略されているが、図1、図3、図4に示すものと同一である。

【0050】記憶メディア1からコンテンツ142を削除する場合は、コンテンツ削除手段81がコンテンツID1421を読み出し、このコンテンツIDを利用可能コンテンツID管理テーブル141から削除し、コンテ

ンツ142を記憶メディア1から消去する。

【0051】ここで不正利用者が記憶メディアAのコンテンツCを磁気ディスクにバックアップし、コンテンツCを記憶メディアAから別の記憶メディアBに移動した後、磁気ディスクのデータを記憶メディアAにリストアした場合には、リストアしたコンテンツのコンテンツIDはメディアAの無効コンテンツID管理テーブルに記録されている。従って第2の実施形態で示した情報利用装置を使ってこのリストアされたコンテンツを読み出すことはできない。つまり、バックアップによる不正利用は防がれているのである。

【0052】

【発明の効果】以上説明したように、本発明によれば、メディアIDとコンテンツIDを結合してメディアコンテンツIDを生成し、目的情報をメディアコンテンツIDで固有化してコンテンツデータを生成し、コンテンツIDとコンテンツデータを組にしたコンテンツを記憶メディアに記録するので、メディアIDをコンテンツIDで暗号化した結果で目的情報を固有化し得るとともに、また予め別のコンテンツ鍵を用意し、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を目的情報として固有化することによりコンテンツの暗号化の処理を軽減することも可能である。

【0053】また、本発明によれば、コンテンツIDが無効コンテンツID管理テーブルに記録されている場合には、目的情報の取得処理を中止し、記録されていない場合には、メディアIDとコンテンツIDを結合してメディアコンテンツIDを生成し、このメディアコンテンツIDでコンテンツのコンテンツデータを一般化して、目的情報を取得するので、無効コンテンツID管理テーブルに記録されているコンテンツの目的情報は取得できないとともに、更にメディアIDをコンテンツIDで暗号化した結果でコンテンツデータを一般化することができ。

【0054】更に、本発明によれば、第1の記憶メディアから第2の記憶メディアに前記コンテンツを移動する際は、コンテンツIDが無効コンテンツID管理テーブルに記録されていないことを確認し、第1の記憶メディアの第1のメディアIDとコンテンツIDを結合して第1のメディアコンテンツIDを生成し、この第1のメディアコンテンツIDでコンテンツのコンテンツデータを一般化して、目的情報を取得し、第2の記憶メディアの第2のメディアIDとコンテンツIDを結合して第2のメディアコンテンツIDを生成し、第1の記憶メディアから取得した目的情報を第2のメディアコンテンツIDで固有化してコンテンツデータを生成し、コンテンツIDとコンテンツデータを組にしたコンテンツを第2の記憶メディアに記録するので、無効コンテンツID管理テーブルに記録されているコンテンツの目的情報は取得できず、従って移動前に予め第1の記憶メディアのコンテ

13

コンテンツをバックアップしてあった場合、移動の際にコンテンツのコンテンツIDは無効にされるため、移動後にバックアップを第1の記憶メディアにコピーして、上述したように読み出して利用しようとしてもコンテンツを読み出すことはできない。すなわち、利用者はバックアップすることはできるが、バックアップしたとしても情報の不正利用は適確に防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

【図2】図1の実施形態で使用する無効コンテンツID管理テーブルのフォーマットを示す図である。

【図3】本発明の第2の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

【図4】本発明の第3の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

【図5】本発明の第4の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

【図6】本発明の第5の実施形態に係るメディア固有化*

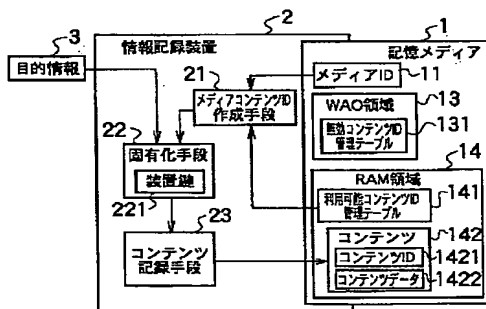
14

*情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

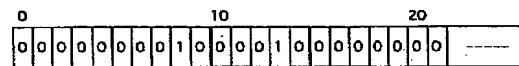
【符号の説明】

- 1 記憶メディア
- 2 情報記録装置
- 3 目的情報
- 4 情報利用手段
- 5 情報移動手段
- 6 バックアップ装置
- 8 削除装置
- 11 メディアID
- 13 WAO領域
- 14 RAM領域
- 21 メディアコンテンツID作成手段
- 22 固有化手段
- 23 コンテンツ記録手段
- 42, 52 一般化手段
- 131 無効コンテンツID管理テーブル
- 141 利用可能コンテンツID管理テーブル
- 142 コンテンツ
- 1421 コンテンツID
- 1422 コンテンツデータ

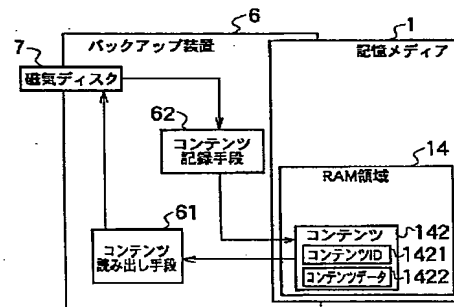
【図1】



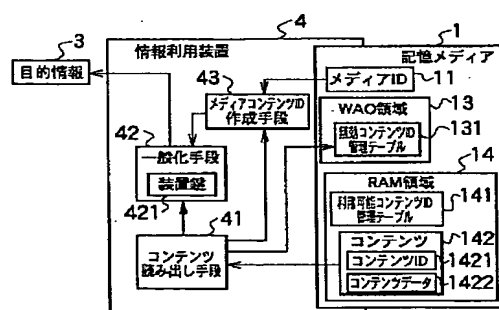
【図2】



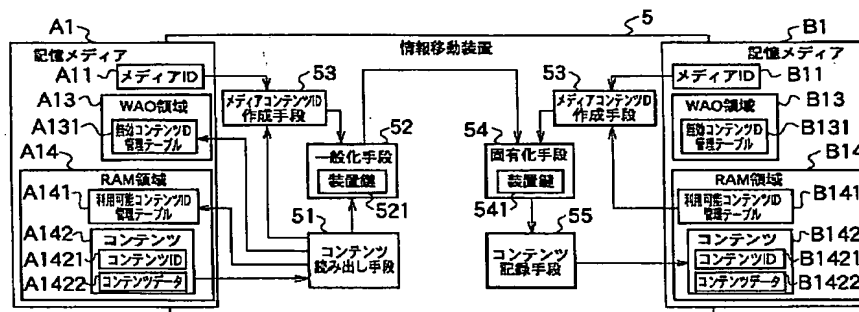
【図5】



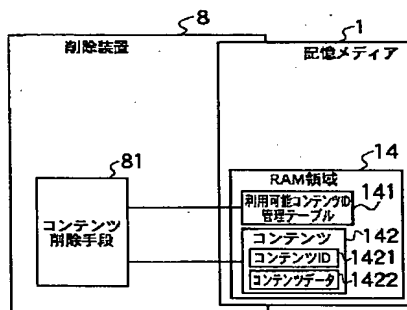
【図3】



【図4】



【図6】



フロントページの続き

Fターム(参考) 5B017 AA06 BA05 BA07 CA06 CA11
CA16
5D110 AA16 AA17 DA02 DA11 DB03
DC28 DD13 DD16 DE04

This Page Blank (uspto)